UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,197	10/31/2003	Pradipta Kumar Banerjee	JP920030162US1	9974

39903 7590 09/27/2007

IBM ENDICOTT (ANTHONY ENGLAND)
LAW OFFICE OF ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
OSMAN, RAMY M	

ART UNIT	PAPER NUMBER
2157	

MAIL DATE	DELIVERY MODE
09/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/698,197	BANERJEE ET AL.	
	Examiner	Art Unit	
	Ramy M. Osman	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) *12,24 and 35* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,13-23 and 25-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is responsive to amendment filed on July 6, 2007, where applicant elected Group I (claims 1-11,13-23 and 25-34) and withdrew claims (12,24,35). Claims 1-11,13-23 and 25-34 are pending examination.

Drawings

2. The drawings filed on 10/31/2003 are acknowledged and are acceptable.

Claim Objections

3. Claims 2,14,26 are objected to for minor informalities:

In line 9 of each respective claim, change "... administrator any data packets are..." to "... administrator **of** any data packets **that** are...".

In line 11 of each respective claim, change "... transport layer terminate..." to "... transport layer **to** terminate...". Appropriate correction is required.

4. Claims 6-8 objected to for minor informalities. The claims have improper dependencies and fail to depend on an independent claim. Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. Claim 35 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim states that "instructions are arranged to detect...". However, instructions in-and-of themselves have no ability to perform the claimed actions of "detect",

"determining", etc. The instructions must be embodied where they are executed by some type of processing system.

Furthermore, applicant is requested to change "computer-readable medium" to "computer-readable storage medium".

The above-mentioned requirements are necessary for the claim to be 101-compliant and for the claim to produce a useful, concrete and tangible result. **(see MPEP 2106 Section IV. C.)**

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 11,23,34 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim states "generating a fake response". However, the meaning of response is a reply to some sort of action, and the claims are silent as to what action is being responded to. Therefore the claims are vague and unclear.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1,3-11,13,15-23,25 and 27-34 rejected under 35 U.S.C. 102(b) as being anticipated by Vaidya (US Patent No 6,279,113).

10. In reference to claim 1, Vaidya teaches a method of detecting an intrusion in a communications network, the method comprising the steps of:

scanning data packets processed by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures (column 6 lines 8-14);

determining if said scanned data packets are malicious (column 6 lines 17-20); and

taking at least one action if any data packets are determined to be malicious (column 6 lines 19-25).

11. In reference to claim 3, Vaidya teaches the method according to claims, further comprising the step of transmitting to said application layer any data packets determined not to be malicious (column 7 lines 4-6).

12. In reference to claim 4, Vaidya teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan module (column 7 lines 4-10).

13. In reference to claim 5, Vaidya teaches the method according to claim 1, wherein at least one application receive queue (ARQ) functions intermediate said transport layer and said application layer (column 7 lines 11-40).

14. In reference to claim 6, Vaidya teaches the method according to claim 7, wherein said scanning step is carried out between said transport layer and said at least one application receive queue (ARQ) (column 7 lines 11-24).

15. In reference to claim 7, Vaidya teaches the method according to claim 6, further comprising the step of obtaining data from said at least one application receive queue (ARQ) (column 7 lines 14-20).

16. In reference to claim 8, Vaidya teaches the method according to claim 7, wherein said scanning step is performed on data packets from said at least one application receive queue (ARQ) (column 7 lines 31-40).

17. In reference to claim 9, Vaidya teaches the method according to claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored (column 7 lines 11-40).

18. In reference to claim 10, Vaidya teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan daemon (column 6 lines 1-10).

19. In reference to claim 11, Vaidya teaches the method according to claim 1, further comprising the step of generating fake responses (column 11 lines 52-65).

20. In reference to claims 13,15-23, these claims are system claims that correspond to the method claims of claims 1,3-11. Therefore, claims 13,15-23 are rejected based upon the same rationale as given for claims 1,3-12 above.

21. In reference to claims 25,27-34, these claims are method claims that correspond to the method claims of claims 1,3-11. Therefore, claims 25,27-34 are rejected based upon the same rationale as given for claims 1,3-12 above.

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. **Claims 2,14,26 rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US Patent No 6,279,113) in view of Copeland (US Patent No 7,185,368).**

In reference to claims 2,14,26, Vaidya teaches the corresponding method, system, and computer-readable medium according to claims 1,13,25 respectively, wherein said at least one action is selected from the group consisting of:

interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol (column 6 lines 21-25);

logging of errors related to any data packets determined to be malicious (column 6 lines 21-25); informing a network administrator any data packets are determined to be malicious (column 6 lines 21-25); intimating said transport layer terminate an existing connection related to any data packets determined to be malicious (column 6 lines 21-25); blocking network access to a source of any data packets determined to be malicious (column 6 lines 21-25); terminating an application of an application layer if any data packets are determined to be malicious (column 6 lines 21-25); and notifying an application of an application layer if any data packets are determined to be malicious (column 6 lines 21-25).

Vaidya fails to explicitly teach modifying firewall rules of a host computer if any data packets are determined to be malicious. However, Copeland discloses an intrusion detection

system that modifies a firewalls behavior by configuring the firewall to drop packets it finds to be malicious for the purpose of protecting a network from the harmful effects of a network intrusion (column 19 lines 20-30 & column 22 lines 40-48).

It would have been obvious for one of ordinary skill in the art to modify Vaidya by modifying firewall rules of a host computer if any data packets are determined to be malicious as per the teachings of Copeland for the purpose of protecting a network from the harmful effects of a network intrusion.

Conclusion

24. The above rejections are based upon the broadest reasonable interpretation of the claims. Applicant is advised that the above specified citations of the relied upon prior art are only representative of the teachings of the prior art, and that any other supportive sections within the entirety of the reference (including any figures, incorporation by references, claims and priority documents) is implied as being applied to teach the scope of the claims.

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramy M. Osman whose telephone number is (571) 272-4008. The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

RMO
September 14, 2007